IT Security Guidelines for Use in BWU Program

1) Context, Purpose, Scope:
   a) The Department of Motor Vehicles (DMV) maintains a computer system to support the operation of its various programs. Within the DMV the Information Security Officer is responsible for maintaining the security of the system. This responsibility includes assuring that the hardware, software and data are used for appropriate purposes only; assuring that the hardware, software and data are not altered except as appropriate; and, assuring the personal, confidential and proprietary information are not accessed, disclosed or used for an inappropriate purpose or in an inappropriate manner.
   b) The DMV permits some persons, generally described as "bonded web users," to access the DMV's information assets to enable the bonded web users to provide services to themselves and their clients as authorized by law. This access may involve: access to personal, confidential or proprietary information; an ability to add, delete or modify information; and, an opportunity to damage DMV information assets. This in turn places the DMV, and the public, at increased risk of damage and misuse of the information assets
   c) Current practice at DMV has been to have programs, such as the Bonded Web User Program within Motor Carrier Division, make the determination as to whether a bonded web user may have access to the DMV computer system, as well as subsequent decisions affecting the DMV/bonded web user relationship after its start. Therefore it is anticipated that these rules will be applied by DMV programs in determining whether or not to permit access and in making subsequent decisions. The Information Security Officer will work internally with DMV programs to apply these rules and other applicable requirements.
   d) These rules shall apply to the operations of bonded web user who are provided access to the DMV computer system to enable them to provide services to themselves and to their clients, in a manner consistent with the purposes for which DMV maintains the computer system.
   e) These rules are a portion the Information Security Officer's security requirements for permitting access to the DMV computer system.
   f) These rules are directed to both an internal DMV audience of DMV programs for whose use the system is primarily maintained and who may provide access to the DMV computer system to bonded web users; and, an external audience of bonded web users and potential bonded web users who may be permitted access to the system to enable them to provide services to their clients.
   g) These rules are subject to change.
   h) Additional requirements may be imposed without alteration of these rules based on the facts of an individual or small number of bonded web users' use of the DMV computer system.
2) These rules apply to bonded web users and bonded web user applicants:
   a) These rules apply to persons who seek to become bonded web users (applicants) and to bonded web users, as those terms are defined in the bonded web user agreement.
   b) These rules do not apply to:
      i) persons who access DMV publicly available information through DMV publicly available portals.
      ii) officers and employees of the department acting in the course of their employment.
      iii) access required by applicable law, to the extent the access required by the law is inconsistent with these rules.
      iv) access ordered by a court of competent jurisdiction, to the extent the order is inconsistent with these rules.

3) Definitions:
   a) "Accountable items" means physical items issued or distributed by DMV and identified by a unique number or other unique identifier, including but not limited to license plates and year stickers.
   b) "Applicant" means a person requesting access to the DMV computer system.
   c) "Bonded web user" means a principal person given access to the DMV computer system by DMV for the purpose of enabling the person to provide services to its clients using the DMV computer system. "Bonded web user" includes but is not limited to a person providing registration services to itself or its clients including the collection and transmission of fees due to DMV, the alteration of DMV records to reflect the transaction, and the delivery of license plates or stickers to itself or its clients. "Bonded web user" does not mean an officer, agent or employee of a "bonded web user."
   d) "Computer systems" means hardware, software, and data, maintained and operated by DMV, including but not limited to subsystems, networks, applications, programs, databases interfaces, and servers.
   e) "Controlled items" means physical things issued or distributed by DMV and kept track of by type of item and volume, but without a unique identifier for each item.
   f) "Individual" means a human being.
   g) "Information assets" means:
      i) automated information including but not limited to, records, files and databases held by the State.
      ii) facilities, equipment and software owned or leased by the state.
   h) "Person" means a human being, a corporation, a limited partnership, or other entity capable of contracting and holding property.
   i) "Personal information" means any information maintained by the DMV that identifies or describes an individual, including but not limited to his name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history, and including statements by or about the individual (see Civil Code section 1798.3).
   j) "Proprietary assets" means all records, files, computer programs and data used to operate DMV, including but not limited to mailing lists, access control tables, printouts, lists, manuals and publications, whether or not protected by copyright or trade secret, on which DMV controls use by others.
   k) "Proprietary information" means computer programs, files and data owned by a person, including a government agency.
   l) "Security incident" means the unauthorized taking, use, release, modification, damage, destruction, disclosure, loss, or access to information assets (see SAM §4845), whether by a DMV officer or employee or some other person, including but not limited to:
      i) taking, use, disclosure, modification, damage, or deletion of information held by or owned by DMV.
      ii) taking, use, release, modification, damage or destruction of equipment or software held by or owned by DMV.
      iii) Occurrence of a computer virus on or in a DMV information asset.
      iv) The presence of unauthorized software on a DMV information asset.
      v) The otherwise authorized use of an information asset in the commission of a crime.
   m) "Workstation" means a specific computer terminal or other device for accessing a computer system.

4) General requirement: A person having access to the DMV computer system:
   a) Shall use that access only for the purposes and in the manner authorized by DMV.
   b) Shall maintain the privacy, security and integrity of the DMV computer system.
   c) Shall prevent the damage or other alteration of DMV hardware, software or data except as authorized by the DMV.
   d) Shall prevent the access, use or dissemination of personal, confidential and proprietary information except as authorized by law and as authorized by DMV.
5) Maintenance of an information technology security program. An applicant or bonded web user having access to DMV information assets shall develop, maintain and implement an information technology security program to protect the DMV assets (computer systems and the information resident thereon) from any and all risks arising out of the giving of access to the applicant or bonded web user, applicable to physical and electronic access to DMV information assets, which will include at least the following elements:
   a) Procedures and practices for the access and use of the information assets, to protect the DMV information assets and information derived from the assets, and assure that they are used only in an appropriate manner.
   b) Worksites which by their arrangement, furnishing, security features and other elements contribute to the security provided for the information assets.
   c) Exclusion of persons not authorized to have access to the DMV information assets from portions of the worksites where workstations, servers and information are located, and where information may be viewed.
   d) Storage of records derived from DMV information assets and resident in a portable medium or method, workstations, printers, and servers, in storage devices which are not readily portable because their size, weight, or method of attachment to the worksite.
   e) Training of employees, agents, and any other person permitted by the bonded web user to have access to information assets, including access to information obtained from the assets, to follow the procedures and practices necessary to protect the information assets and assure that they are used only in an appropriate manner.
   f) Record-keeping for all transactions attempted or performed using the DMV information assets; all workstations used to access the DMV information assets; all individuals permitted access to the system or the information derived from the system.
   g) Active detection, recording, reporting, analysis and remediation of security incidents.
   h) Compliance with this agreement and other applicable laws relating to the protection of the State's information assets or the interests of persons in their personal, confidential and proprietary information.
   i) Providing a detailed description of the information technology security program to DMV.
   j) Subsequent reconsideration and modification of the information technology security program.
6) Documentation of the bonded web users' information technology security program; modification; obligation to follow.
   a) An applicant for access to the DMV information assets shall provide the DMV as a part of the application process with a detailed written description of its information technology security program.
   b) The DMV may grant or refuse an application for access or limit access granted based on the adequacy of the information security program description submitted. The procedures for considering and making a determination on an application are set forth in the rules governing the administration of individual DMV programs.

c) A bonded web user shall comply with the information security program description provided as part of the application process unless and until a proposed modification of the program has been submitted to the DMV and DMV has approved the modification. A bonded web user shall comply with the program as modified once a program modification has been approved.

d) The DMV may end, limit, or place conditions on a bonded web user's access to the information assets based on the bonded web user's compliance with its information technology program. The procedures for considering and making a determination on ending, limiting, or placing conditions on a bonded web user's access to the information assets are set forth in the rules governing the administration of individual DMV programs.

7) Information Security and Disclosure Statement, Public/Private Partnerships Employee form. A bonded web user shall require any individual to be provided access to the DMV information assets by the bonded web user, including any agent and employee of the bonded web user, to complete and sign an information security and disclosure statement, on an "Information Security and Disclosure Statement, Public/Private Partnerships Employee" form (EXEC200x). The completed and signed form shall be maintained by the bonded web user while the individual has access to the DMV computer system and for three years following the last time the individual has access. The form shall be made available to the State, including DMV, upon request, for purposes of inquiry, audit or investigation.

8) Individuals permitted access only after notification to the department. The bonded web user shall permit an individual to access the DMV information assets through the bonded web user's access only after the bonded web user has obtained, from the individual, a completed and signed "Information Security and Disclosure Statement, Public/Private Partnerships Employee" form (EXEC200x). The bonded web user shall not permit an individual to access the DMV information assets through the bonded web user's access when the bonded web user has been notified by DMV that the individual is not to be permitted access.

9) The bonded web user's information security program shall include:
   a) Diagrams illustrating the floor plan of each worksite, including the location of walls, doors, windows, workstations, equipment, storage devices and furniture, at which the bonded web user permits access to the DMV information assets.
   b) A narrative description of features of the worksite which provide security to the DMV information assets, including but not limited to alarm systems, video surveillance, window and door locks.
   c) A narrative description of safes, file cabinets, desks, and other furniture used in connection with taking access to the DMV information assets or storage of data derived from the assets.
   d) A narrative description of processes and procedures to prevent members of the public, clients, or other individuals from being exposed to personal, confidential or proprietary information other than as appropriate.

10) Record of individuals provided access.
   a) The bonded web user shall maintain a record of each individual it intends to permit, permits, or has permitted access to the DMV information assets. The record shall include for each individual:
      i) The individual's name.
      ii) The individual's address.
      iii) The individual's driver license number or identification card number and the issuing state.
      iv) The individual's birth date.
      v) The individual's user identifier for purposes of taking access.
      vi) The period of time during which the individual was permitted access.

vii) The workstations through which the individual was permitted access.
viii) The locations at which the individual was permitted access.

b) The bonded web user shall maintain the record of an individual provided access for a period of three years from the last time the individual is permitted or has taken access. The bonded web user shall make the record available to the State, including DMV, upon request, for purposes of inquiry, audit or investigation.

11) Record of Workstations.
   a) A bonded web user shall maintain a record of all workstations through which it has, or has had, access to the DMV computer system. The record shall include:
      i) The make, model and serial number of the device.
      ii) For each location where the device is maintained while capable of access, the physical location and the period during which the device was or is maintained at that location.
      iii) For each individual presently or previously provided or permitted access to the device by the bonded web user, the identity of the individual and the period or periods of time during which the individual had access to the device. The identity provided shall be sufficient to identify the individual in the bonded web user's record of employees provided access.
   b) The bonded web user shall maintain the workstation record while the workstation is capable of access to the DMV computer system and for three years following the last time the device is capable of access. The record shall be made available to the State, including DMV, upon request, for purposes of inquiry, audit or investigation.
12) Record of transactions.
   a) A bonded web user shall maintain a record of all transactions conducted through the use of its access. The record shall include:
      i) The date of the transaction.
      ii) The identification of the workstation used in the transaction.
      iii) The identification of the individual operating the workstation for the transaction.
      iv) The type of transaction.
      v) The identifiers used to identify any vehicle or any individual affected by the transaction.
   b) The bonded web user shall retain the record of work stations while the workstation is set up to access and for three years after the workstation is no longer set up to access. The record shall be made available to the State, including DMV, upon request for purposes of inquiry, audit or investigation.
13) Audit. The bonded web user shall permit the State, including DMV, to conduct audits, as determined necessary by the State or DMV, to determine the bonded web user's compliance with these information technology security guidelines. The bonded web user shall make available to the State, including DMV, its facilities, hardware, software, records, and personnel for the purpose of facilitating the conduct of an audit under this section.
14) Security Incident reporting. A bonded web user, as part of its information technology protection program, shall notify the DMV Information Security Officer, and any other person required by the department to be notified, within one (1) state business day of discovery of facts or information tending to indicate the occurrence of a security incident involving a DMV information asset. The notice shall be in writing and contain:
   a) The identity of the bonded web user, and the bonded web user's address and telephone number.
   b) The date, time, and physical location of the incident.
   c) The identity of any workstation or other machine or device involved in the incident.
   d) The name, address and telephone number of each witness to the incident, including any individuals who may have caused the incident.
   e) A narrative description of the incident.

f) A narrative description of any steps being taken by the bonded web user to remediate any damage.
g) A narrative description of any steps being taken by the bonded web user to prevent a recurrence of the sort of incident.

15) Passwords, credentials, authentication.
   a) A bonded web user shall maintain as a part of its information technology protection program a system of protective measures limiting access to the DMV computer system which requires each user upon each access attempt to enter a user identifier and a password prior to obtaining access.
   b) Each user shall select his own password. A password must consist of a combination at least eight number and character figures, including at least one number figure and at least one character figure. A user shall select a password which does not make use of his own name, his own initials, his own social security number, or that of one of his family members.
   c) A password shall be manually entered. A password shall not be entered by any automated method.
   d) A password shall not be written or displayed in any plain text readable format.
   e) A user shall not disclose his password to another person.
   f) A user shall change his password at least once every 60 days.
   g) A user shall not reuse a password previously used within any consecutive 12 iterations.
16) A bonded web user may propose an information technology protection program which differs from that prescribed by the bonded web user agreement. The DMV will consider any varying information protection security program proposed by a bonded web user, and may approve a varying information technology program if the program, in the judgment of the DMV, provides equal or greater protection to the DMV information assets.

I certify that I have read, understand, agree, and will comply with the IT Guidelines for Use in BWU Program.

_____
Company Name of BWU Program Applicant

_____ _____ _____
Printed Name of Authorized Employee Title Date

_____
Signature of Authorized Employee

Please return to the BWU Program Administrator at:

DEPARTMENT OF MOTOR VEHICLES
Motor Carrier Division
Bonded Web User Program
P.O. Box 932345 MS H825
Sacramento, CA 94232-3700